



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/560,788	04/28/2000	Wesley A. Witt	2480	5145

7590 11/04/2004

Law Offices Of Albert S. Michalik, PLLC
704-228th Ave. NE
Suite 193
Sammamish, WA 98074

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT PAPER NUMBER

2131

DATE MAILED: 11/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/560,788	Applicant(s) WITT ET AL.	
	Examiner Christopher A. Revak	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6-17, 19-24, 26-35, 37-39 and 46-49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-17, 19-24, 26-35, 37-39 and 46-49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) * | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Upon further consideration of the teachings of Krishnaswami et al, the examiner interprets the teachings to meet the applicant's claim limitations. PROSECUTION IS HEREBY RE-OPENED.

Double Patenting

2. Claims 1,20,31, and 46-48 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1,10,12, and 15 of U.S. Patent No. 6,618,735. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1,20,31, and 46-48 of the instant application are envisioned by patent claims 1,10,12, and 15 in that claims 1,10,12, and 15 of the patent contains all the limitations of claims 1,20,31, and 46-48. Claims 1,20,31, and 46-48 of the instant application therefore are not patentably distinct from the earlier patent claims and as such, are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4,6-17,19-24,26-35,37-39 and 46-49 are rejected under 35

U.S.C. 102(e) as being anticipated by Krishnaswami et al.

As per claim 1, it is disclosed by Krishnaswami of a computer system comprising a method for receiving information indicative of a possible change to a protected file and determining whether the change is valid by verifying the file. The verifying is performed by a verifying mechanism and if not valid, preventing the change that includes discarding the change data and returning a success to a component (col. 1, line 64 through col. 2, line 5 and col. 10, lines 2-10). The teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file (col. 5, lines 3-6).

As per claim 2, it is taught by Krishnaswami of receiving information indicative of a possible change that includes receiving notification indicative of a change to a protected file (col. 9, line 49 through col. 10, line 17).

As per claim 3, Krishnaswami discloses of receiving information indicative of a possible change including the reception of a notification of a change to a file and accessing information to determine if the file is protected (col. 9, line 49 through col. 10, line 17).

As per claim 4, it is taught by Krishnaswami that the change is prevented by overwriting a changed copy of the file with a valid copy of the protected file (col. 5, lines 3-6).

As per claim 6, Krishnaswami discloses that it is determined whether the file is valid by verifying the file based on a cryptographic hash of the information and comparing the cryptographic hash information against cryptographic hash information associated with the protected file (col. 6, line 60 through col. 7, line 8).

As per claim 7, it is further disclosed by Krishnaswami that the cryptographic hash includes accessing a catalog of information for protected files (col. 6, line 60 through col. 7, line 8).

As per claim 8, it is disclosed by Krishnaswami of determining whether a change is valid that includes determining whether the file includes a cryptographic hash (col. 6, line 60 through col. 7, line 8). It is interpreted that the cryptographic hash is also referred to as a signature since they are both mathematical functions used to produce identifying values for comparison.

As per claim 9, it is taught by Krishnaswami monitoring files in a file system (col. 10, lines 18-21).

As per claim 10, Krishnaswami teaches of preventing the change includes copying a valid copy of the protected file to a former location of the protected file (col. 9, lines 30-35).

As per claim 11, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file (col. 6, line 60 through col. 7, line 8 and col. 9, lines 30-35).

As per claim 12, it is taught by Krishnaswami of finding a file having the same identity as the protected file includes accessing a temporary directory (cache)(col. 5, lines 31-38, col. 6. line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 13, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file (col. 6, line 60 through col. 7, line 8 and col. 9, lines 30-35).

As per claim 14, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file includes accessing a network (col. 3, lines 47-49, col. 6, line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 15, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file (col. 6, line 60 through col. 7, line 8 and col. 9, lines 30-35).

As per claim 16, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file includes accessing a medium (col. 3, lines 13-28, col. 6, line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 17, Krishnaswami discloses of copying a valid copy of the protected file includes finding a file having the same identity as the protected file (col. 6, line 60 through col. 7, line 8 and col. 9, lines 30-35).

As per claim 19, Krishnaswami teaches of receiving information indicative of a change to a protected file that is about to be changed, preserving a copy of the protected file and preventing the change includes overwriting a changed copy of the file with a copy of the protected file that was preserved (col. 1, line 64 through col. 2, line 5, col. 5, lines 3-6, col. 9, lines 30-35, and col. 10, lines 2-10).

As per claim 20, Krishnaswami discloses of a computer readable medium having computer readable instructions for selecting a plurality of files as protected files. Information is receiving that indicates a possible change to a protected file. It is determined whether it is an exception case and if an exception case, allowing the change, or if not an exception case, determining whether the change is valid by verifying the file, which is performed by a verification mechanism. If valid, allowing the change and if not valid, preventing the change and returning information indicative of a success (col. 1, line 64 through col. 2, line 5, col. 5, lines 29-40, and col. 10, lines 2-10).

As per claim 21, it is taught by Krishnaswami of receiving information indicative of a possible change that includes receiving notification indicative of a change to a protected file (col. 9, line 49 through col. 10, line 17).

As per claim 22, Krishnaswami discloses of receiving information indicative of a possible change including the reception of a notification of a change to a file and

accessing information to determine if the file is protected (col. 9, line 49 through col. 10, line 17).

As per claim 23, it is taught by Krishnaswami that the change is prevented by overwriting a changed copy of the file with a valid copy of the protected file (col. 5, lines 3-6).

As per claim 24, the teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file (col. 5, lines 3-6).

As per claim 26, Krishnaswami discloses of allowing the change includes writing the data saved via a copy-on-write process to the file (col. 9, lines 38-45).

As per claim 27, it is taught by Krishnaswami of determining whether the file is an exception case includes checking a certificate (security descriptor) of the file (c col. 1, line 64 through col. 2, line 5, col. 5, lines 29-40, and col. 9, lines 36-45).

As per claim 28, Krishnaswami discloses of providing a prompt before allowing the change (col. 10, lines 2-10).

As per claim 29, Krishnaswami discloses that it is determined whether the file is valid by verifying the file based on a cryptographic hash of the information and comparing the cryptographic hash information against cryptographic hash information associated with the protected file (col. 6, line 60 through col. 7, line 8).

As per claim 30, it is disclosed by Krishnaswami of determining whether a change is valid that includes determining whether the file includes a cryptographic hash (col. 6, line 60 through col. 7, line 8). It is interpreted that the cryptographic hash is also

referred to as a signature since they are both mathematical functions used to produce identifying values for comparison.

As per claim 31, it is taught by Krishnaswami of a computer system comprising a protected file, a detection mechanism configured to determine when the protected file may be changed, a verification mechanism, and a file protection service. The file protection service is configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the change is valid and to prevent the change by discarding the changed data when the change is not valid (col. 1, line 64 through col. 2, line 5 and col. 9, line 49 through col. 10, line 17). The teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file (col. 5, lines 3-6).

As per claim 32, Krishnaswami discloses of a detection mechanism that includes a mechanism for monitoring at least one directory for changes to a file (col. 1, line 64 through col. 2, line 5 and col. 6, lines 25-27).

As per claim 33, it is taught by Krishnaswami that a detection mechanism provides a notification to the file protection service as the determination mechanism that detects that the protected file may be changed (col. 9, line 49 through col. 10, line 17).

As per claim 34, Krishnaswami teaches of a file protection service that accesses a data structure to determine whether the notification received from the detection mechanism corresponds to a protected file (col. 9, line 49 through col. 10, line 17).

As per claim 35, Krishnaswami discloses of a file protection service that is incorporated into a file system (col. 10, lines 18-21).

As per claim 37, it is taught by Krishnaswami that a file protection service returns information indicative of a success (col. 9, line 49 through col. 10, line 17).

As per claim 38, Krishnaswami discloses that it is determined whether the file is valid by verifying the file based on a cryptographic hash of the information and comparing the cryptographic hash information against cryptographic hash information associated with the protected file (col. 6, line 60 through col. 7, line 8).

As per claim 39, Krishnaswami discloses of a cryptographic hash associated with a valid file is maintained in a data structure including a cryptographic hash of the contents of one other protected file (col. 6, line 60 through col. 7, line 8).

As per claim 46, is taught by Krishnaswami of a computer system comprising a protected file, a detection mechanism configured to determine when the protected file may be changed, a verification mechanism, and a file protection service. The file protection service is configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the change is valid and to prevent the change by discarding the changed data when the change is not valid (col. 1, line 64 through col. 2, line 5 and col. 9, line 49 through col. 10, line 17). The teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file (col. 5, lines 3-6). The change is

prevented by locating valid data in a system temporary directory (cache) and copying the valid data over the changed data when the change is not valid (col. 5, lines 31-38, col. 6, line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 47, it is taught by Krishnaswami of a computer system comprising a protected file, a detection mechanism configured to determine when the protected file may be changed, a verification mechanism, and a file protection service. The file protection service is configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the change is valid and to prevent the change by discarding the changed data when the change is not valid (col. 1, line 64 through col. 2, line 5 and col. 9, line 49 through col. 10, line 17). The teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file by checking and locating the valid data in a network share (col. 3, lines 47-49, col. 5, lines 3-6, col. 6, line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 48, it is taught by Krishnaswami of a computer system comprising a protected file, a detection mechanism configured to determine when the protected file may be changed, a verification mechanism, and a file protection service. The file protection service is configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the change is valid and

to prevent the change by discarding the changed data when the change is not valid (col. 1, line 64 through col. 2, line 5 and col. 9, line 49 through col. 10, line 17). The teachings of Krishnaswami disclose of undoing the change and the examiner is interpreting the undoing of the change as being that of discarding the change data since the change is undone to restore the original file (col. 5, lines 3-6). Valid data is located in a recording medium and the data is undone (copied back) to the original form when the change is not valid (col. 3, lines 13-28, col. 6, line 60 through col. 7, line 8, and col. 9, lines 30-35).

As per claim 49, it is disclosed by Krishnaswami that a scanning mechanism causes files to trigger the detection mechanism (col. 9, line 49 through col. 10, line 17).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.


Haerder et al, "Principles of Transaction-Oriented Database Recovery"

Blakely, "Security Requirements for DCE"


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

November 1, 2004

Christopher Revak
AU 2131


11/1/04